(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2002372910 A

(43) Date of publication of application: 26.12.02

(51) Int. Cl G09C 1/00
G06F 12/14
H04N 5/91
H04N 5/93

(21) Application number: 2001182956

(22) Date of filing: 18.06.01

(71) Applicant: VICTOR CO OF JAPAN LTD

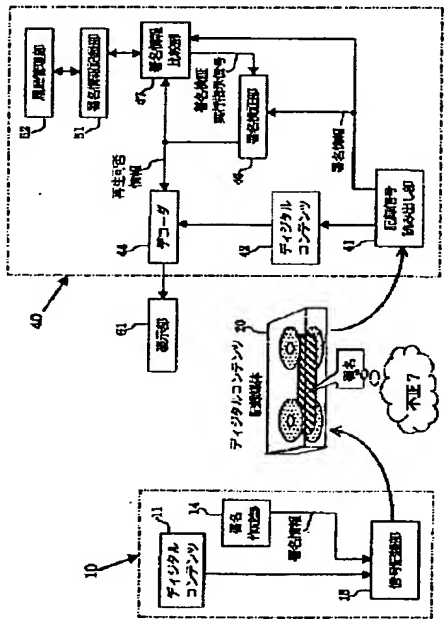
(72) Inventor: SUGAWARA TAKAYUKI
SHICHIJO SHUNICHI

(54) AUTHENTICATING AND REPRODUCING METHOD FOR CONTENTS INFORMATION AND CONTENTS INFORMATION AUTHENTICATING AND REPRODUCING DEVICE

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a contents reproducing device extracting contents to which unauthorized signature information is attached by verifying a signature and denying its reproduction and reproducing only digital contents to which right signature information is attached by a simple signature verification.

SOLUTION: By collating signature information recorded on a recording medium together with the digital contents with the unauthorized signature information to be an unauthorized object stored in a storage medium beforehand, when matching information is present, the reproduction of the contents is denied or stopped without performing the processing of authentication. Also, when the matching unauthorized signature information is not present, the signature information is verified. When it is verified as the unauthorized signature information, the unauthorized content information is additionally stored in the storage medium as the unauthorized signature information and the reproduction of the contents is stopped.



(19) 日本国特許庁 (JP)　　(12) 公開特許公報（A）　　(11) 特許出願公開番号

特開２００２－３７２９１０
(P２００２－３７２９１０A)
(43) 公開日　平成14年12月26日(2002.12.26)

(51)Int.Cl.[7]		識別記号	FI			テーマコード'(参考)
G09C	1/00	640	G09C	1/00	640 Z	5B017
		660			660 D	5C053
G06F	12/14	320	G06F	12/14	320 A	5J104
H04N	5/91		H04N	5/91	P	
	5/93			5/93	Z	

審査請求　未請求　請求項の数　１０　ＯＬ　（全 １５ 頁）

(21) 出願番号　特願2001-182956(P2001-182956)

(22) 出願日　平成13年6月18日(2001.6.18)

(71) 出願人　000004329
日本ビクター株式会社
神奈川県横浜市神奈川区守屋町3丁目12番地

(72) 発明者　音原　隆幸
神奈川県横浜市神奈川区守屋町3丁目12番地　日本ビクター株式会社内

(72) 発明者　七條　俊一
神奈川県横浜市神奈川区守屋町3丁目12番地　日本ビクター株式会社内

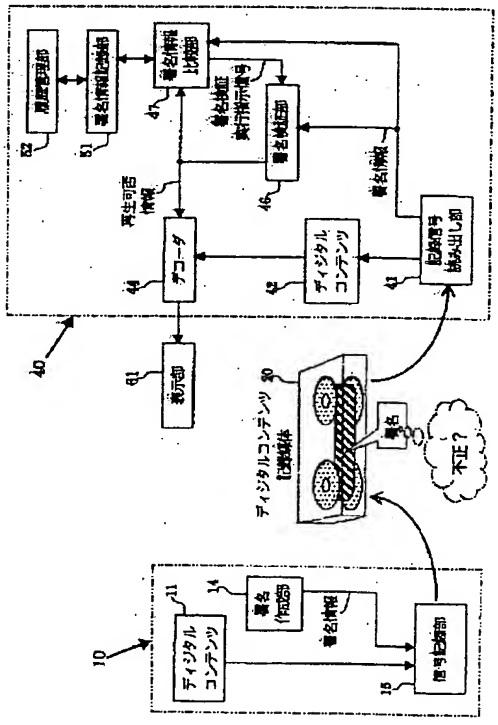
Ｆターム(参考)　5B017　AA07　CA16
5C053　FA13　FA22　FA25　GA11　GB37
HA40　JA21
5J104　AA07　AA09　KA01

(54)【発明の名称】コンテンツ情報の認証再生方法、及びコンテンツ情報認証再生装置

(57)【要約】

【課題】　不正な署名情報が付されるコンテンツを署名検証することにより抽出して再生を不許可とし、正当な署名情報が付されるディジタルコンテンツのみを再生するコンテンツ再生装置を簡易な署名検証により実現することにある。

【解決手段】　記録媒体にディジタルコンテンツと共に記録される署名情報を、予め記憶媒体に記憶した不正対象となる不正署名情報と照合することにより、一致する情報が存在するときは認証の処理を行わずにコンテンツの再生を不許可もしくは停止するようにし、また一致する不正署名情報がないときはその署名情報を検証して不正な署名情報として検証されたときは、その不正コンテンツ情報を不正署名情報として記憶媒体に追加記憶すると共に、そのコンテンツの再生を停止するようにして実現した。



1

【特許請求の範囲】

【請求項１】正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とを記録したディジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報の認証再生方法であって、

前記ディジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る第１のステップと、

正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する第２のステップと、

その第２のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第３のステップと、

前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第４のステップと、

を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【請求項２】正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とが伝送されるディジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報の認証再生方法であって、

前記ディジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る第１のステップと、

正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する第２のステップと、

その第２のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第３のステップと、

前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第４のステップと、

を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【請求項３】正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とを記録したディジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報認証再生装置であって、

2

前記ディジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る記録信号読み出し手段と、

正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段と、

その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段と、

前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段と、

を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【請求項４】正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とが伝送されるディジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報認証再生装置であって、

前記ディジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る情報信号受信手段と、

正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段と、

その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段と、

前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段と、

を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【請求項５】前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、取

り外し可能な可搬型記憶媒体である前記署名情報記録手段に記憶された前記不正署名情報群を用いて行うことを特徴とする請求項３又は４記載のコンテンツ情報認証再生装置。

【請求項６】前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、ネットワークに接続されるネットワークサーバの記憶媒体に記憶される前記不正署名情報群のデータを得、その得られたデータを用いて行うことを特徴とする請求項３又は４記載のコンテンツ情報認証再生装置。

【請求項７】前記署名検証手段における署名検証は、前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段を有するネットワークサーバに、前記再生署名情報をネットワークを介して伝送すると共に、前記ネットワークサーバより前記署名検証の結果に係る情報を得て行うことを特徴とする請求項３又は４記載のコンテンツ情報認証再生装置。

【請求項８】前記署名検証手段における前記ディジタルコンテンツの再生中止に係る動作は、そのディジタルコンテンツ情報の復号を行う復号器に、再生が不許可であることを示す再生不可情報を供給して復号を中止する動作であることを特徴とする請求項３又は４記載のコンテンツ情報認証再生装置。

【請求項９】前記署名検証手段における前記ディジタルコンテンツの再生中止に係る動作は、前記ディジタルコンテンツに付されるコピー許可情報がコピー許可であるとされる場合であっても、そのコピーのためのディジタルコンテンツ信号の他の記録媒体への供給を中止する動作であることを特徴とする請求項３又は４記載のコンテンツ情報認証再生装置。

【請求項１０】前記署名情報記録手段における前記再生署名情報の前記不正署名情報群への追加は、可搬型である記憶媒体に追加記憶するようになすことを特徴とする請求項３又は４記載のコンテンツ情報認証再生装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ディジタルコンテンツ及びそのディジタルコンテンツを記録した記録媒体の認証再生方法に関するもので、特に不正な署名情報の検証方法、及びそのディジタルコンテンツが再生されたときの処理方法、更にその方法を搭載した装置に関する。

【０００２】

【従来の技術】従来より、著作権で保護されるディジタルコンテンツが、不正にコピーされた記録媒体の利用を防止するための有効な手段として、署名による認証を行う方法が一般的になされている。その認証再生方法は、記録媒体に、ディジタルコンテンツの他に、その記録媒体あるいはコンテンツが正当なものであることを示す署名情報を記録し、その署名情報を基にコンテンツ再生の許可、不許可を与えるようにしてコンテンツの再生制御を行うものである。

【０００３】そのディジタルコンテンツの再生制御が行われる装置では、まずその署名が正当なものであるかどうかが検証され、正当なものであるとされるときにのみディジタルコンテンツの再生が行なわれるようにしている。

【０００４】そして、特開２０００－２２６８０号公報「ディジタルコンテンツ流通方法及びコンテンツを再生可能に記録した記録媒体」には、署名の検証結果を基に、少なくとも一部を暗号化したディジタルコンテンツの復号化に必要な鍵を復号化するかどうかを判断し、署名等の情報が有効であると判断されたときにコンテンツを復号する方法が開示されており、そのような署名によりコンテンツ再生の制御を行う方法は知られている。

【０００５】

【発明が解決しようとする課題】しかしながら、上記の方法で用いられるような署名を用いる方式では、署名情報の改竄等に対する保護に一定以上のセキュリティレベルを確保しようとするときに、署名及びその署名の保護に係る必要なデータ量は大きくなり、かつ署名の認証に用いられる演算量も多くなり、その認証処理は複雑になる。

【０００６】そして、その署名の認証を行うためには十分な処理能力のあるパソコンを用いて行う等の信号処理のための作業環境が必要であるが、一般のユーザが利用可能なディジタルコンテンツ再生装置にはそのような処理能力の高いコンピュータシステムを搭載することは再生装置の価格が高価になり好ましくなく、通常は署名認証のための処理能力が低くされる場合が多い。

【０００７】そのような処理能力の低い署名認証機能しか有しないディジタルコンテンツ再生装置では、ユーザによる再生操作がなされた後にコンテンツが再生されて表示されるまでには多くの時間が必要とされ、しかもそのような複雑な署名認証処理をコンテンツの再生毎に行わなければならなく、そのようなディジタルコンテンツ再生装置は再生動作が開始されてからコンテンツが表示されるまでに時間を要してしまうなど、使い勝手の良い機能を実現するために障害となるなどの課題があった。

【０００８】そこで、本発明は、コンテンツ及びそのコンテンツを記録した記録媒体が、正当なコンテンツ及び記録媒体であることを示す署名情報を記録した記録媒体から情報を再生するに際し、コンテンツ及び記録媒体の認証を行い、不正なコンテンツ及び媒体であると認められたときはコンテンツの再生を不許可もしくは停止するようなディジタルコンテンツ再生方法において、記録媒体に記録される認証情報を、予め記憶媒体に記憶される不正対象となる署名情報と照合し、一致する情報が存在するときは前記認証の処理を行わずに、コンテンツの再

生を不許可もしくは停止するようにした。

【０００９】また、一致する情報が存在しないときは、その新しいコンテンツ及び記録媒体の署名に係る認証作業を行い、不正なコンテンツ及び媒体であると認証された場合には、その不正対象となる署名情報を、取り外し可能なメディア、ないしはメモリ素子に記憶する、又はその署名情報をネットワークインターフェースを介してネットワークに接続されるサーバシステムの記憶装置に記憶するようにして、予め記憶媒体に記憶される不正対象となる署名情報の更新を行なうようにし、コンテンツ再生の際に行われる署名情報の認証作業が簡略化されたコンテンツ情報の認証再生方法、及びその方法を搭載するコンテンツ情報認証再生装置の構成を提供しようとするものである。

【００１０】

【課題を解決するための手段】本発明は、上記課題を解決するために以下の１）～１０）の手段より成るものである。すなわち、

【００１１】１）　正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とを記録したディジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報の認証再生方法であって、前記ディジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る第１のステップ（４１）と、正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する第２のステップ（４７）と、その第２のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第３のステップ（４６）と、前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第４のステップ（５１）と、を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【００１２】２）　正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とが伝送されるディジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報の認証再生方法であって、前記ディジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る第１のステップ（４９）と、正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちの

いずれかと一致するか否かを検出する第２のステップ（４７）と、その第２のステップにより前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う第３のステップ（４６）と、前記署名検証により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する第４のステップ（５１）と、を少なくとも有することを特徴とするコンテンツ情報の認証再生方法。

【００１３】３）　正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とを記録したディジタルコンテンツ記録媒体のみを再生するためのコンテンツ情報認証再生装置であって、前記ディジタルコンテンツ記録媒体を再生して前記署名情報に係る再生署名情報を得る記録信号読み出し手段（４１）と、正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段（４７）と、その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ記録媒体の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段（４６）と、前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段（５１）と、を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【００１４】４）　正当な権利の基に制作されたディジタルコンテンツと、そのディジタルコンテンツの制作者の認証に係る署名情報とが伝送されるディジタルコンテンツ伝送情報のみを再生するためのコンテンツ情報認証再生装置であって、前記ディジタルコンテンツ伝送情報を再生して前記署名情報に係る再生署名情報を得る情報信号受信手段（４９）と、正当な権利の基でなく制作されたディジタルコンテンツに付された不正署名情報を累積記憶した不正署名情報群と、前記再生署名情報とを比較して前記再生署名情報が前記不正署名情報群のうちのいずれかと一致するか否かを検出する署名情報比較手段（４７）と、その署名情報比較手段により前記不正署名情報と一致した前記再生署名情報が検出されたときは前記ディジタルコンテンツ伝送情報の再生を中止するための信号を供給し、また前記不正署名情報との一致が検出

されないときは前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段（４６）と、前記署名検証手段により前記再生署名情報の正当性が検証されないときは、その再生署名情報を前記不正署名情報群に追加記憶する署名情報記録手段（５１）と、を少なくとも具備して構成することを特徴とするコンテンツ情報認証再生装置。

【００１５】５）　前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、取り外し可能な可搬型記憶媒体である前記署名情報記録手段に記憶された前記不正署名情報群を用いて行うことを特徴とする３）又は４）項記載のコンテンツ情報認証再生装置。

【００１６】６）　前記署名情報比較手段における前記再生署名情報との比較に用いられる前記不正署名情報群は、ネットワークに接続されるネットワークサーバの記憶媒体に記憶される前記不正署名情報群のデータを得、その得られたデータを用いて行うことを特徴とする３）又は４）項記載のコンテンツ情報認証再生装置。

【００１７】７）　前記署名検証手段における署名検証は、前記再生署名情報が前記ディジタルコンテンツの制作者の認証に係る署名情報であるか否かの署名検証を行う署名検証手段を有するネットワークサーバに、前記再生署名情報をネットワークを介して伝送すると共に、前記ネットワークサーバより前記署名検証の結果に係る情報を得て行うことを特徴とする３）又は４）項記載のコンテンツ情報認証再生装置。

【００１８】８）　前記署名検証手段における前記ディジタルコンテンツの再生中止に係る動作は、そのディジタルコンテンツ情報の復号を行う復号器に、再生が不許可であることを示す再生不可情報を供給して復号を中止する動作であることを特徴とする３）又は４）項記載のコンテンツ情報認証再生装置。

【００１９】９）　前記署名検証手段における前記ディジタルコンテンツの再生中止に係る動作は、前記ディジタルコンテンツに付されるコピー許可情報がコピー許可であるとされる場合であっても、そのコピーのためのディジタルコンテンツ信号の他の記録媒体への供給を中止する動作であることを特徴とする３）又は４）項記載のコンテンツ情報認証再生装置。

【００２０】１０）　前記署名情報記録手段における前記再生署名情報の前記不正署名情報群への追加は、可搬型である記憶媒体に追加記憶するようになすことを特徴とする３）又は４）項記載のコンテンツ情報認証再生装置。

【００２１】

【発明の実施の形態】以下、本発明のコンテンツ情報の認証再生方法、及びコンテンツ情報認証再生装置の実施の形態につき、好適な実施例により説明する。図１は、そのコンテンツ情報の認証再生方法を搭載するコンテンツ情報認証再生装置を含むコンテンツ情報認証記録再生システムの概略ブロック図であり、その構成と動作について概説する。

【００２２】同図に示すコンテンツ情報認証記録再生システムは、ディジタルコンテンツ部１１、署名作成部１４、及び信号記録部１５よりなるコンテンツ情報認証記録装置１０と、ディジタルコンテンツ記録媒体２０と、表示部６１と、そしてコンテンツ情報認証再生装置４０とより構成される。

【００２３】そして、そのコンテンツ情報認証再生装置４０は、記録信号読出し部４１、ディジタルコンテンツメモリ４２、デコーダ４４、署名検査部４６、署名情報比較部４７、署名情報記録部５１、及び履歴管理部５２より構成される。

【００２４】次に、そのように構成されるコンテンツ情報認証記録再生システムの動作について概説する。まず、例えばＭＰＥＧ（moving picture experts group）により策定された符号化方式により圧縮符号化されたビットストリームなどのディジタルコンテンツ部１１に蓄積されるディジタルコンテンツは、署名作成部１４により暗号化されて生成された署名情報と共に信号記録部１５に供給され、そこでディジタルビデオテープなどのディジタルコンテンツ記録媒体２０にそれらの供給された信号の記録がなされる。

【００２５】このようにして記録されたディジタルコンテンツ記録媒体２０は、正規の著作権の保護されるディジタルコンテンツが、著作権者に係る署名情報と共に記録されたものであるが、そのディジタルコンテンツ記録媒体２０が不法コピーされて記録されたディジタルコンテンツ記録媒体２０の署名情報は、署名作成部１４により暗号化されて生成された署名情報とは異なる不正な署名情報として記録されるようになされる。

【００２６】このようにして記録されたディジタルコンテンツ記録媒体２０は、コンテンツ情報認証再生装置４０によりディジタルコンテンツ及び署名情報の再生、とその復号がなされるが、次にそのコンテンツ情報認証再生装置４０の動作について述べる。

【００２７】まず、ディジタルコンテンツ記録媒体２０は記録信号読出し部４１により再生され、再生されて得られるディジタルコンテンツはディジタルコンテンツメモリ４２に、また署名情報は署名検査部４６及び署名情報比較部４７に供給される。

【００２８】その署名情報比較部４７では、予め署名情報記録部５１に記録されている不正な署名情報テーブルと供給された署名情報とが比較され、不正な署名情報と一致する署名情報が検出されたとき、その検出結果に係る再生不可情報はデコーダ４４に供給され、そのデコーダ４４ではディジタルコンテンツメモリ４２に一時記憶されたディジタルコンテンツの復号動作が中止される。

【００２９】一方、署名情報比較部４７に供給された署名情報と、予め署名情報記録部５１に記録されている不正な署名情報テーブルとで一致する署名情報の検出がなされないときは、その署名情報比較部４７では署名検査部４６に対して署名検証実行指示信号が供給され、その署名検査部４６では供給された署名情報の正当性について後述の暗号解析手法により署名情報の検証が行われる。

【００３０】そして、署名情報が正当であると検証されたときは、デコーダ４４に対して再生許可を与えるための再生可否情報が供給され、デコーダ４４ではディジタルコンテンツメモリ４２に一時記憶されるコンテンツ情報は、例えばＭＰＥＧ標準により圧縮符号化のなされているディジタルコンテンツはそこでＭＰＥＧ標準に基づいて復号化がなされ、復号化されて得られる映像信号は表示部６１に供給されて、そのコンテンツの内容が表示される。

【００３１】このようにして正当であるとして検証されたコンテンツの内容は表示されるが、反対に署名検証部４６で署名情報が不正であるとして判定されたときは、ディジタルコンテンツの復号を中止するための再生可否情報がデコーダ４４に供給されて復号動作が中止されると共に、その判定された署名判定情報は署名情報比較部４７に供給され、その署名情報比較部４７では不正として判定された署名情報を署名情報記録部５１に供給し、その署名情報記録部５１では供給された署名情報は不正な署名情報テーブルに追加記録される。

【００３２】そして、その署名情報記録部５１に接続される履歴管理部５２では、署名情報記録部５１の不正な署名情報テーブルに追加記録される署名情報の記録日時、ないしは記録順に係る情報が記録履歴情報として記憶されるが、そのときに署名情報記録部５１での記録量が所定の記録容量に近くなり、記録空き容量が所定値よりも少なくなったときは、例えば古い署名情報より順に消去がなされるようにされて記録領域が確保される。

【００３３】このようにして、記録される署名情報テーブルが用いられることにより、署名検証部４６でなされる署名検証のための処理時間が短縮されると共に、不正な署名情報テーブルに記録される不正なディジタルコンテンツの再生は、直ちにディジタルコンテンツ記録媒体２０の再生、及びその表示が中止されるようになされる。

【００３４】このようにして、コンテンツ情報認証再生装置４０では、ディジタルコンテンツ記録媒体２０に記録されるディジタルコンテンツ、及び過去に再生されて記憶されている不正な署名情報を基にして、コンテンツ内容の再生可否に係る制御を短時間で行うと共に、不正な署名が検出されたときは不正な署名情報テーブルにその署名情報を追加するようにして、更に不正な署名情報に係る制御時間の短縮を図るものである。

【００３５】以上、コンテンツ情報認証再生装置４０の構成と動作について概説したが、更にその構成及び動作について述べる。図２に、実施例１によるコンテンツ情報認証記録再生システムの構成を示し、その動作について述べる。そして、その図２に示すシステムは前述の図１に示したシステムに機能を追加したものであり、次にその追加された機能を主に詳述する。

【００３６】同図に示すコンテンツ情報認証記録再生システムはコンテンツ情報認証記録装置１０ａ、ディジタルコンテンツ記録媒体２０、表示部６１、そしてコンテンツ情報認証再生装置４０ａよりなっており、情報認証記録装置１０ａは前述の情報認証記録装置１０に比してコピー制御フラッグ設定部１２及びハッシュ関数演算部１３が多く含まれて構成され、またコンテンツ情報認証再生装置４０ａは前述のコンテンツ情報認証再生装置４０に比してハッシュ関数部４３、制御部４５、及び外部出力制御部４８が多く含まれて構成されている。

【００３７】次に、そのように構成されるコンテンツ情報認証記録装置１０ａ、ディジタルコンテンツ記録媒体２０、及びコンテンツ情報認証再生装置４０ａの機能及び動作について更に述べる。

【００３８】まず、ディジタルコンテンツ部１１に蓄積されているディジタルコンテンツはＭＰＥＧなどにより圧縮符号化された映像信号の他にも、ＭＰＥＧ以外の方式により符号化された画像信号、符号化音声信号、及びコンピュータプログラムなどの、いわゆるディジタル化された情報信号が用いられる。

【００３９】そのようなディジタル化された情報信号は信号記録部１５に供給されてディジタルコンテンツ記録媒体２０に記録されるが、そのディジタルコンテンツ記録媒体２０はディジタルＶＴＲ用の磁気テープの他に、ディジタルデータを記録するストリーマ用などの磁気テープ、光磁気ディスク、ＤＶＤなどの光ディスク、更には半導体メモリなどのディジタル信号を記録できる記録媒体が用いられる。

【００４０】そのようなディジタルコンテンツ記録媒体２０に記録されるディジタルコンテンツは、コンテンツ情報認証再生装置４０ａにより再生が目的とされて使用されるが、そのコンテンツが他の記録装置に供給されてコピーされるなどの再利用に関しても管理される。

【００４１】そのディジタルコンテンツの再利用に係る制御は、コピー制御フラッグ設定部１２により設定されるコピー制御フラッグにより管理される様になされており、そのコピー制御フラッグは信号記録部１５に供給されて、ディジタルコンテンツ記録媒体２０に記録される。

【００４２】そのディジタルコンテンツ記録媒体２０に記録されるコピー制御フラッグは、記録媒体２０に記録されたディジタルコンテンツの他の記録媒体へのディジタルコピーを許可するか否かを示すフラッグであり、そ

のフラッグにより例えばＣＧＭＳ（Copy Generation Management System）の手法が用いられてコピーの世代が１である「子」まで許すか、ないしは２である「孫」まで許すかなどの許可情報が、コピー制御フラッグ設定部１２により設定される。

【００４３】そのようにして設定されてディジタルコンテンツ記録媒体に記録される情報として署名情報と署名設定フラッグ情報があるが、次にその署名情報及び署名設定フラッグ情報の生成について述べる。

【００４４】その署名情報は、ディジタルコンテンツ記録媒体２０に記録されるコンテンツの正当性を示すものであり、ディジタルコンテンツ部１１に記憶される情報の一部がハッシュ関数演算部１３に供給され、そのハッシュ関数演算部１３ではハッシュ関数などの一方向性関数が用いられて演算されてメッセージダイジェスト（以下ＭＤとする）が得られ、その得られたＭＤは署名作成部１４に供給される。

【００４５】その署名作成部１４では、供給されたＭＤはコンテンツの著作権者により管理される秘密鍵データが用いられ、例えばＲＳＡ（Rivest Shamir Adelmanの３教授により開発された公開鍵暗号方式）署名方式、ないしはＤＳＳ（Digital Signature Standard）署名方式により作成される。

【００４６】そしてその署名作成部１４では、署名情報と共に、その署名情報が記録されているか否かを示す署名情報フラッグ、例えば1ビットのバイナリデータで"0"は署名情報無し、"1"は署名情報ありを示す情報が作成され、それらの作成された署名情報及び署名情報フラッグは信号記録部１５に供給される。

【００４７】以上のようにして、信号記録部１５にはディジタルコンテンツ、コピー制御フラッグ、署名情報、及び署名情報フラッグなどの信号が供給され、それらの供給された信号はディジタルコンテンツ記録媒体２０に記録される。

【００４８】そのようにしてコンテンツ情報認証記録装置１０ａにより記録されたディジタルコンテンツ記録媒体２０はコンテンツ情報認証再生装置４０ａにより再生、及び復号化がなされるが、次にそのコンテンツ情報認証再生装置４０ａによる再生動作について述べる。

【００４９】まず、ディジタルコンテンツ記録媒体２０に記録されたディジタル信号は記録信号読み出し部４１により読み出され、読み出された信号のうちディジタルコンテンツに係る信号はディジタルコンテンツ部４２に、署名情報及び署名情報フラッグの両者は署名検証部４６及び署名情報比較部４７の両方に、またコピー制御フラッグ情報は外部制御出力部４８にそれぞれ供給される。

【００５０】そして、それらの供給される情報の内の署名情報フラッグが"0"である場合は、ディジタルコンテンツ記録媒体２０には署名情報が記録されていないことが示されているので、署名検証部４６では署名情報の検証が行われる必要はなく、署名検証部４６ではデコーダ４４に再生が許可されるための再生可否情報が供給される。

【００５１】一方、署名情報フラッグが"1"であるときは、署名情報が記述されていることが示されており、その署名情報フラッグの供給された署名情報比較部４７では、前述の図１を基に述べたと同様の方法により、供給される署名情報は予め署名情報記録部５１に記録されている不正な署名情報テーブルと比較され、一致する署名情報が検出されたときは再生不可とされる情報が制御部４５に供給される。

【００５２】また、一致する署名情報が検出されないときは、署名検証部４６に署名検証実行指示情報が供給される。そして、その指示情報の供給された署名検証部４６では、ディジタルコンテンツ部４２に一時記憶されたディジタルコンテンツの、所定のコンテンツ情報部分がハッシュ関数処理部によりハッシュ関数処理がなされてＭＤ（Message Digest）信号として供給され、その供給されたＭＤ信号と検証の対象となる署名情報とは署名検証部４６で著作権者により管理される公開鍵が用いられて検証動作がなされる。

【００５３】その検証動作の結果、署名情報が正当であるとして検証されたときは、ディジタルコンテンツ部４２に供給されたディジタルコンテンツ情報はデコーダ４４に供給されて復号され、復号のなされた情報信号は表示部６１に供給されて表示されるなどの、通常の再生動作がなされる。

【００５４】反対に、検証動作の結果署名情報が不正であるとして検証されたときには、ディジタルコンテンツ記録媒体は不正であるとして、署名検証部４６より制御部４５に再生不可とされる再生可否情報が制御部４５を介してデコーダ４４に供給され、デコーダ４４ではディジタルコンテンツの復号動作が中止されると共に、その不正として検証された署名情報は署名情報記録部５１に供給され、そこに記録されている不正な署名情報テーブルに追加記録される。

【００５５】そして、その署名情報記録部５１に追加記録される不正署名情報の書き込みは履歴管理部５２により管理がなされ、不正署名情報記録可能な領域が所定量以上であるときはそこに不正署名情報が記録され、記録領域が所定量以下であるときは、例えば最も古い不正認証情報が消去され、新しく供給される不正認証情報が記録されるようになされる。

【００５６】さらに、このような不正署名情報が検出されたときは、表示部６１に「ディジタルコンテンツ記録媒体２０は不正な記録媒体である」ことを表示し、ユーザにその検証の状況を知らせるようにする。

【００５７】このようにして、ディジタルコンテンツ記録媒体２０に記録されたディジタルコンテンツは、署名

情報、署名情報フラッグの検証が行われることにより、署名情報が記録されていないとき、及び署名情報の検証が正常になされたときにのみコンテンツ情報認証再生装置４０ａより復号された信号が表示部６１に供給されて表示されるようになされている。

【００５８】そして、また、そのコンテンツ情報認証再生装置４０ａには、記録信号読み出し部４１により読み出されたディジタルコンテンツ記録媒体２０の信号は外部出力制御部４８を介して他の記録装置に供給され、コピー記録がなされるような機能が有されている。

【００５９】その外部出力制御部４８では、ディジタルコンテンツ記録媒体２０より読み出されたコピー制御フラッグ信号が供給されており、そのコピー制御フラッグ信号の内容、及び前記署名情報の検証結果に応じて他の記録装置に供給される信号の供給又は非供給の制御がなされる。

【００６０】即ち、ディジタルコンテンツ記録媒体２０に記録されるディジタルコンテンツ、コピー制御フラッグ、及び署名情報が他の記録装置に供給されてディジタルコピーがなされるのは、そのコピー制御フラッグにコピー許可に係る情報があるときのみであり、そのときにディジタルコンテンツ信号及び付随される情報が他の記録装置に供給されるようになされている。

【００６１】そして、前記のような不正署名情報が検出されたときには、記録信号読み出し部４１より外部出力制御部４８にコピー許可に係るコピー制御フラッグが、例えコンテンツがディジタルコピー可能、又は１回だけコピー可能とされている場合であっても、ディジタルコンテンツ等に係る情報が外部記録装置に供給されないように、記録信号読み出し部４１より供給されるコピー制御フラッグはコピー禁止に係るフラッグに変更される。

【００６２】次に、そのようにしてなされるコピー制御について述べる。図３に、コピー制御に係る信号記録の処理をフローチャートにより示し、説明する。

【００６３】まず、ステップ１（Ｓ１）により、コピー制御フラッグ設定部１２でコピー制御フラッグの設定がなされているか否かがチェックされ、設定されていないときはステップ３（Ｓ３）の署名の設定ステップに、またＳ１においてコピー制御フラッグ設定がなされているときはステップ２（Ｓ２）によりコピー制御フラッグの設定を行った後にＳ３の署名設定のステップに移る。

【００６４】そのＳ３では、署名作成部１４において署名の設定が行われた後にコンテンツ、署名情報、署名情報フラッグ、及びコピー制御フラッグの記録のステップ４に移行し、そのステップ４では信号記録部１５によりそれらの信号のディジタルコンテンツ記録媒体２０への記録動作がなされる。

【００６５】次に、その記録されたディジタル記録コンテンツ読み出しの動作について述べる。図４に、そのディジタル記録コンテンツ記録媒体の読み出し制御に係る

信号再生の処理をフローチャートにより示し、説明する。

【００６６】まず、ステップ１１において記録されるコピー制御フラッグの検出が行われ、ステップ１２においてそのコピー制御フラッグによりコピーが許可されているか否かがチェックされ、コピー可能とされるときはステップ１３によりそのフラッグの内容が更新されて、外部出力制御部４８より外部記録装置への信号記録のための信号供給が行われ、次のステップ１５に移行する。

【００６７】そして、Ｓ１２における判定結果がコピー不可とされるときは、ステップ１４により外部記録装置への出力が禁止され、署名情報フラッグの検出ステップ１５に移行し、記録媒体２０に記録される署名情報フラッグの検出が行われる。

【００６８】そして、ステップ１６においてその検出された署名情報フラッグが“１”であるか否かがチェックされ、“１”でないときは記録コンテンツ記録媒体の読み出し制御に係る処理が終了されてディジタルコンテンツ記録媒体２０の再生動作が開始されると共に、検出された署名情報フラッグが“１”であるときはステップ１７による署名情報の読み出しがなされる。

【００６９】そのステップ１７で読み出された署名情報はステップ１８で、既に記憶されている不正署名テーブルに無いかどうかが比較され、不正署名情報があるとき（Ｎｏのとき）はステップ２２に移りコンテンツの再生が停止され、一致する不正署名情報が無いとき（Ｙｅｓのとき）はステップ１９の署名情報の検証動作がなされる。

【００７０】そのステップ１９でなされた検証結果を基に、ステップ２０の署名検証によりコンテンツが正当か否かが判定され、正当であるときはコンテンツ記録媒体の読み出し制御に係る処理が終了されてディジタルコンテンツ記録媒体２０の再生動作が開始されると共に、正当でないと判定されるときはステップ２１により不正署名情報が署名情報記録部５１に供給されて不正署名メモリテーブルに追加記録され、ステップ２２でディジタルコンテンツ記憶媒体の再生が停止される。

【００７１】以上のようにして、ディジタルコンテンツ記録媒体２０に記録されたコピー制御フラッグ、署名情報、及び署名情報フラッグ情報を基にして、記録されるコンテンツの再生、復号動作、及びそのコンテンツの外部接続機器へのコピーのための制御動作が行われる。

【００７２】そして、その不正な署名情報は、予め署名情報記録部に記録される不正署名情報リストとの比較を行うことにより、不正な署名情報は演算が複雑である署名情報検証の作業を行わずに容易に得ることができるものである。

【００７３】そこで、署名情報記録部５１及び履歴管理部５２に記録される不正署名テーブルに係る情報は取り外し可能な例えばフロッピディスク、ないしはＩＣメモ

リ素子などの記憶媒体に記録され、このコンテンツ情報認証再生装置４０ａとは異なるコンテンツ情報認証再生装置の署名情報記録部に、その記憶媒体に記憶された内容を記憶媒体と共に移動してコピーすることにより、その異なるコンテンツ情報認証再生装置は不正署名テーブルに記憶される署名情報を基に容易に不正署名の検出動作が行なわれる。

【００７４】そして、このような不正署名の検出動作は、署名情報フラッグに「署名情報が有り」とされる署名情報フラッグとして読み出されるときに行われる。そこで、仮に署名情報フラッグに記録される「署名情報が有り」の情報が、「署名情報が無し」として改竄されて供給されるときには不正署名の検出動作は行われないことになる。

【００７５】従って、署名情報フラッグのディジタルコンテンツ記録媒体への記録はただ単にコンテンツ情報のヘッダ領域に記録するなどのような簡単な記録方法ではなく、コンテンツ情報の中にその署名フラッグ情報を埋め込むようにして記録する必要がある。

【００７６】即ち、その記録された署名情報の有り無しに係る署名情報フラッグ情報は、例えばコンテンツの中にウオーターマーク情報としてを埋め込むようにして行い、その記録された署名情報フラッグが署名情報有りから署名情報無しに変更されるような場合は、コンテンツの内容自体に破綻が生じ、そのコンテンツが正常に復号されて、表示されることがないようにする方法などが有る。

【００７７】そのようなコンテンツの保護を行なうために、コンテンツ情報認証記録装置はコンテンツの少なくともその一部を暗号化して記録するようにし、コンテンツ情報認証再生装置ではその暗号化されたコンテンツを復号化して再生するようにする方法により実現することができる。

【００７８】即ち、そのような暗号化されたコンテンツに署名情報有り無しに係る署名情報フラッグを埋め込み、その情報フラッグが改竄されたときに暗号化信号の解読がなされないように構成するのは比較的容易である。

【００７９】以上、第１の実施例におけるコンテンツ情報認証記録装置によりディジタルコンテンツ記録媒体に記録したディジタルコンテンツの認証、及びコンテンツ情報の復号動作について述べたが、そのディジタルコンテンツは記録媒体に記録されて搬送される外に、通信路、ないしは放送伝送路が用いられて直接伝送されるようなディジタルコンテンツ情報に関しても同様なコンテンツ情報認証伝送受信システムを構成することができる。

【００８０】図５に、コンテンツ情報認証伝送再生システムの構成を示す。同図に示す第２の実施例によるコンテンツ情報認証伝送装置１０ｂは、前述のコンテンツ情

報認証記録装置１０ａに比して信号記録部１５が伝送装置１６に、またディジタルコンテンツ記録媒体２０は伝送路３０になっている点で異なっている。

【００８１】そして、コンテンツ情報認証再生装置４０ｂはコンテンツ情報認証再生装置４０ａに対して記録信号読み出し部４１が受信装置４９とされて構成されるがその他の構成は同一であり、従ってコンテンツ情報認証伝送再生システムは記録媒体の代りにディジタル伝送媒体を用いてディジタルコンテンツの配信を行う点で異なっており、その他の動作は前述の第１の実施例におけるコンテンツ情報認証記録装置と同様である。

【００８２】このようにして、第１の実施例で示したコンテンツ情報認証記録再生システムにおけるディジタルコンテンツの認証、及びコンテンツ情報の復号動作については第２の実施例で示すコンテンツ情報認証伝送再生システムにおいても同様に行われる。

【００８３】そして、第２の実施例ではディジタルコンテンツ記録媒体２０の代りに伝送路３０が用いられているが、その伝送路は署名情報記録部に記録された不正署名情報テーブルの伝送に使用することもできる。

【００８４】図６に、その不正署名情報テーブルを記憶する記憶媒体をネットワークサーバ５０に設け、不正署名情報は伝送ネットワークを介して伝送する、ないしはネットワークを介して取得する場合のコンテンツ情報認証再生装置４０ｃの構成を示し説明する。

【００８５】同図に示すコンテンツ情報認証再生装置４０ｃは、前述の図５におけるコンテンツ情報認証再生装置４０ｂの構成に比して署名情報記録部５１及び履歴管理部５２はなく、署名検証部４６はネットワークインタフェース３１及び３２を介して、ネットワークサーバ５０の中にある署名情報記録部５１及び履歴管理部５２が接続されている。

【００８６】そのように接続される署名検証部における不正署名情報の検証は、前述の図２に示した署名検証部４６と同様に行われ、検証作業により不正なコンテンツ及び媒体であると認められた場合には、その作業の行われたコンテンツ情報認証再生装置における再生可否情報は再生不許可もしくは再生停止の指示信号を制御部４５に供給されると共に、その検証された不正署名情報はネットワークインタフェース３１、及び３２を介してネットワークサーバ５０の署名情報記録部５１に供給される。

【００８７】そして、その不正署名情報は、ネットワークサーバ５０にネットワーク接続される複数のコンテンツ情報認証再生装置により共有されるようになされ、その不正署名情報リストは複数のコンテンツ情報認証再生装置により共用して利用されると共に、それぞれのコンテンツ情報認証再生装置により検証された不正署名情報のそれぞれはそのネットワークサーバ５０に供給される。

【００８８】そのネットワークサーバ５０には複数のコンテンツ情報認証再生装置により検出された多くの不正署名情報が供給されて、短期間に不正署名情報に係るデータベースが構築されることとなり、各々のコンテンツ情報認証再生装置による検証作業が減少される。

【００８９】そして、そのデータベースを記憶するネットワークサーバの署名情報記録部の容量は大きく設定されるが、その署名情報記録部に供給される不正署名情報は履歴管理部５２によりなされており、署名情報記録部５１における不正署名情報記録領域に記録可能とされる空き領域があるときは、その不正署名情報は署名情報記録部に記録され、記録可能な領域が不足している場合には、例えば最も古い不正認証情報が消去され、新しく供給された不正認証情報が記録されるようになされる。

【００９０】そのようにして記録される不正認証情報は、前述の第１の実施例におけるコンテンツ情報認証再生装置の場合では、不正署名情報リストをフロッピディスク、ないしはＩＣメモリ素子を介して異なるコンテンツ情報認証再生装置の間でデータの共有を行なうようにしていたが、ネットワーク結合による不正署名データの共有は、新たに検証された不正署名データに対するデータの更新が実時間で、且つ記憶媒体の交換作業を伴わなく容易になされるため、それぞれのコンテンツ情報認証再生装置における署名データ検証のための作業を削減することができるものである。

【００９１】以上、ネットワークサーバ５０に署名情報記録部５１を有し、不正署名データを共有する第３の実施例について述べたが、次にそのネットワークサーバに署名検証部を設ける場合の例について述べる。

【００９２】図７は、そのネットワークサーバに署名検証部を設ける場合の第４の実施例によるコンテンツ情報認証再生装置の構成を示したものであり、それらの動作について説明する。

【００９３】即ち、同図に示すコンテンツ情報認証再生装置４０ｄは、前述の図６に示した第３の実施例によるコンテンツ情報認証再生装置４０ｃに比し、署名検証に係るハッシュ関数部４３、署名検証部４６、及び署名情報比較部４７の回路部がないが、それらはネットワークインタフェース３１ａ及びネットワークインタフェース３１ｂを介してネットワークサーバ５０ａの中にあるハッシュ関数部４３、署名検証部４６、及び署名情報比較部４７に接続されるようになされて構成されている点で異なっている。

【００９４】このように構成されるコンテンツ情報認証再生装置４０ｄの動作は、コンテンツ情報認証再生装置４０ｃの動作に比し、署名の検証に係る動作が必要なときはネットワークを介してネットワークサーバ５０ａに検証作業を要求し、そのサーバー部５０ａでは検証作業により得られた結果に応じ、コンテンツ情報認証再生装置４０ｄに関する再生可否情報はネットワークを介して

制御部４５に供給されると共に、不正な署名情報に関しては前述と同様にして署名情報記録部５１にその不正署名情報の記録が行なわれようにされる。

【００９５】即ち、コンテンツ情報認証再生装置４０ｄよりネットワークサーバ５０ａに署名情報、署名情報フラッグ、及びディジタルコンテンツのメッセージダイジェストを作成するために必要なコンテンツの一部の情報は、ネットワークインタフェース３１ａを介してネットワークサーバ５０ａに供給され、そのネットワークサーバ側ではネットワークインタフェース３２ａを介して供給されるそれらの情報信号を得て署名の認証作業が行なわれるようにする。

【００９６】このようにして、ネットワークを介して行う署名認証作業用の信号、及び再生可否情報などは、ネットワークに接続される他のコンピュータにより改竄される可能性が有るので、ネットワークを介して伝送される信号は十分に強度の高い暗号化がなされていることが望ましい。

【００９７】そして、ネットワークサーバ５０ａでは、署名情報記録部に記録される不正署名データが外部からのアクセスにより消去される、あるいは正当な署名情報が不正署名情報として記録されるなどのような改竄がなされることを防止するためにも十分に保護される暗号化システムにより構成することが望ましいが、その他に記録された不正署名データの再検証を定期的に行うなどによる記憶データの維持管理が必要である。

【００９８】以上、第１～第４の実施例により、記憶される不正署名データを用いて高速且つ容易に署名情報の検証を行う記録再生方法、伝送受信方法、及びそれらを搭載する装置の構成、及びそれらの動作について述べた。

【００９９】それらの記録及び伝送装置により署名情報、及び署名フラッグ情報が付されたディジタルコンテンツ情報の再生、ないしは受信に際し、そのディジタルコンテンツと記録媒体、ないしは伝送媒体で伝送される署名情報の認証を行い、不正なコンテンツ及び媒体であると検証されたときには、その再生を中止すると共に、再度その不正署名情報を有する媒体が再生されようとされるときは、前記認証の処理を行うことなくコンテンツの再生を不許可もしくは停止させることができ、処理時間の短縮、及び処理の簡易化ができる。

【０１００】そして、その不正署名情報は、特に取り外し可能な記録媒体ないしはメモリ素子にその不正署名情報を記録するようにしたので、それらの不正署名情報記録媒体ないしはメモリ素子を複製し、複数の再生装置ないしは受信装置にそれらの不正署名情報記録媒体を供給することにより複数の装置で署名認証のための作業の高速化、および簡易化がなされる。

【０１０１】また、複数の再生装置ないしは受信装置をネットワークにより結合し、ネットワークを介して不正

署名情報の供給を行う場合には、複数の装置のうちの１つの装置により検証された不正署名情報を同時に共有することができるため、更に簡便に署名情報が検証されて動作する再生装置ないしは受信装置を構成することができる。

【０１０２】さらに、ネットワーク上に接続されているネットワークサーバに不正署名情報を検証して得、その得られた不正署名情報を記録するようにしたので、ネットワークに接続される全ての再生装置ないしは受信装置は、署名情報の検証機能を有していない場合であっても高演算機能を備えたネットワークサーバにより検証された署名情報を基にディジタルコンテンツの再生、ないしは受信を行なうことができる認証処理速度が早く、且つ低価格であるコンテンツ情報認証再生装置を構成することができるものである。

【０１０３】

【発明の効果】請求項１記載の発明によれば、正当な権利の基に制作されたディジタルコンテンツに、そのディジタルコンテンツの制作に係る署名情報が付加されて記録されたディジタルコンテンツ記録媒体を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたディジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはディジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【０１０４】また、請求項２記載の発明によれば、正当な権利の基に制作されたディジタルコンテンツに、そのディジタルコンテンツの制作に係る署名情報が付加されて伝送されたディジタルコンテンツ情報を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたディジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはディジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報認証再生方法を提供できる効果がある。

【０１０５】また、請求項３記載の発明によれば、正当な権利の基に制作されたディジタルコンテンツに、そのディジタルコンテンツの制作に係る署名情報が付加されて記録されたディジタルコンテンツ記録媒体を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたディジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはディジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理手段を簡易に構成できると共に認証処理時間を削減したコンテンツ情報認証再生装置の構成を提供できる効果がある。

【０１０６】また、請求項４記載の発明によれば、正当な権利の基に制作されたディジタルコンテンツに、そのディジタルコンテンツの制作に係る署名情報が付加されて伝送されたディジタルコンテンツ情報を再生するに際し、再生して得られる再生署名情報を予め記憶した不当な権利に基づき制作されたディジタルコンテンツに付された複数の不正署名情報が格納される不正署名情報テーブルと比較して不正署名情報を検出し、不正署名情報が検出されたときはディジタルコンテンツ記録媒体の再生を中止し、また不正署名情報が検出されないときは再生署名情報の正当性の検証に係る署名検証を行い、正当性が検証されないときはその再生署名情報を不正署名情報テーブルに追加して記憶するようにしているため、複雑な演算処理による認証処理を行う頻度を少なくすることができ、認証処理に係る処理手段を簡易に構成できると共に認証処理時間を削減したコンテンツ情報認証再生装置の構成を提供できる効果がある。

【０１０７】また、請求項５記載の発明によれば、請求項３及び４記載の効果に加え、特に署名比較は、取り外し可能な可搬型記憶媒体に記憶された不正署名情報テーブルを用いて行うようにしているため、更に認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【０１０８】また、請求項６記載の発明によれば、請求項３及び４記載の効果に加え、特に署名比較は、ネットワークに接続されるネットワークサーバの記憶媒体をアクセスし、その記憶媒体に記憶される不正署名情報テーブルのデータを用いて行うにしているため、認証処理に係る処理工程を更に簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【０１０９】また、請求項７記載の発明によれば、請求

項３及び４記載の効果に加え、特に署名検証は、ネットワークに接続され再生署名情報の正当性の検証機能を有するネットワークサーバに、再生署名情報を伝送し、そのネットワークサーバより再生署名情報の正当性の検証結果に係る署名検証情報はネットワークを介して得られるようにしているため、さらに認証処理に係る処理工程を簡易にできると共に認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【０１１０】また、請求項８記載の発明によれば、請求項３及び４記載の効果に加え、特にディジタルコンテンツ再生の中止に係る動作は、圧縮符号化されたディジタルコンテンツ情報の復号を行う復号器に、再生が不許可であることを示す再生不可情報を供給するようにしているため、認証処理に係る処理工程に係る遅延時間のために誤って復号化されたディジタルコンテンツ情報が再生されてしまうといったような誤動作を防止したコンテンツ情報の認証再生方法を提供できる効果がある。

【０１１１】また、請求項９記載の発明によれば、請求項３及び４記載の効果に加え、特に記録媒体の再生の中止に係る動作は、ディジタルコンテンツ記録媒体に、その記録されるディジタルコンテンツが他の記録媒体にコピーすることを許可するコピー許可情報が記録されている場合であっても、そのコピーのための信号供給を中止する動作を同時に行うことによりコピー許可に係る誤動作を防いだコンテンツ情報の認証再生方法を提供できる効果がある。

【０１１２】また、請求項１０記載の発明によれば、請求項３及び４記載の効果に加え、特に再生署名情報の不正署名情報テーブルへの追加は、可搬型の記憶媒体に追加記憶するようにしているため、その記憶された不正署名情報テーブルは他のコンテンツ情報の認証再生方法に用いることができるため、その認証方法を搭載するコンテンツ情報の認証再生装置に係る認証処理の処理工程を簡易にできると共に、認証処理時間を削減したコンテンツ情報の認証再生方法を提供できる効果がある。

【図面の簡単な説明】

【図１】本発明のコンテンツ情報認証再生装置に係るコンテンツ情報認証記録再生システム構成の概略を示す図である。

【図２】本発明の第１の実施例に係るコンテンツ情報認証記録再生システムの構成を示す図である。

【図３】本発明の実施例によるコンテンツ情報認証記録装置に係る記録信号の動作を示すフローチャートである。

【図４】本発明の実施例によるコンテンツ情報認証再生装置に係る再生信号の動作を示すフローチャートである。

【図５】本発明の第２の実施例に係るコンテンツ情報認証記録再生システムの構成を示す図である。

【図６】本発明の第３の実施例に係るコンテンツ情報認証再生装置の構成を示す図である。

【図７】本発明の第４の実施例に係るコンテンツ情報認証再生装置の構成を示す図である。

【符号の説明】

１０、１０ａ　コンテンツ情報認証記録装置

１０ｂ　コンテンツ情報認証伝送装置

１１　ディジタルコンテンツ部

１２　コピー制御フラッグ設定部

１３　ハッシュ関数演算部

１４　署名作成部

１６　伝送装置

２０　ディジタルコンテンツ記録媒体

３０　伝送路

３１、３１ａ、３２、３２ａ　ネットワークインタフェース

４０、４０ａ、４０ｂ、４０ｃ、４０ｄ　コンテンツ情報認証再生装置

４１　記録信号読出し部

４２　ディジタルコンテンツメモリ

４３　ハッシュ関数部

４４　デコーダ

４５　制御部

４６　署名検査部

４７　署名情報比較部

４８　外部出力制御部

４９　受信装置

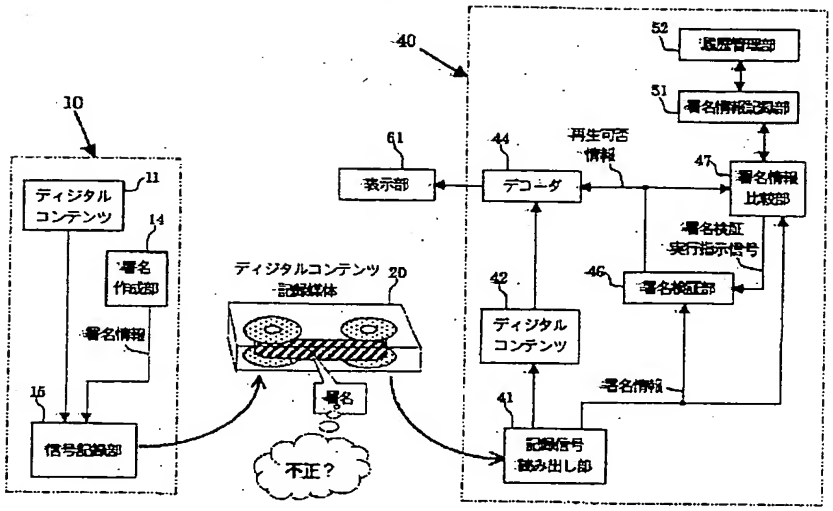
５０、５０ａ　ネットワークサーバ

５１　署名情報記録部

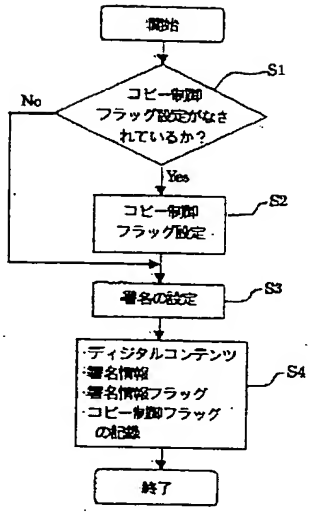
５２　履歴管理部

６１　表示部

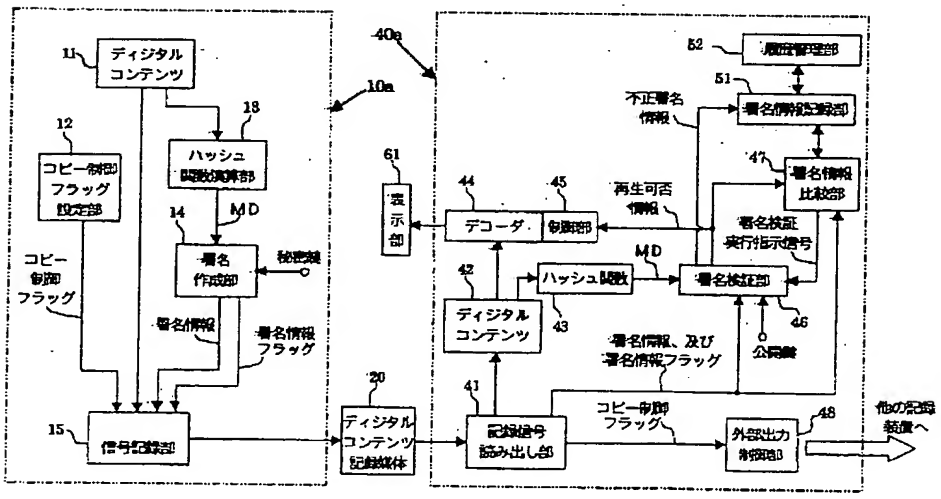
【図１】


10
ディジタルコンテンツ
11
署名作成部
14
署名情報
15
信号記録部
ディジタルコンテンツ記録媒体
20
署名
不正？
40
52
履歴管理部
51
署名情報記憶部
61
表示部
44
再生可否情報
デコーダ
47
署名情報比較部
署名検証実行指示信号
46
署名検証部
42
ディジタルコンテンツ
署名情報
41
記録信号読み出し部

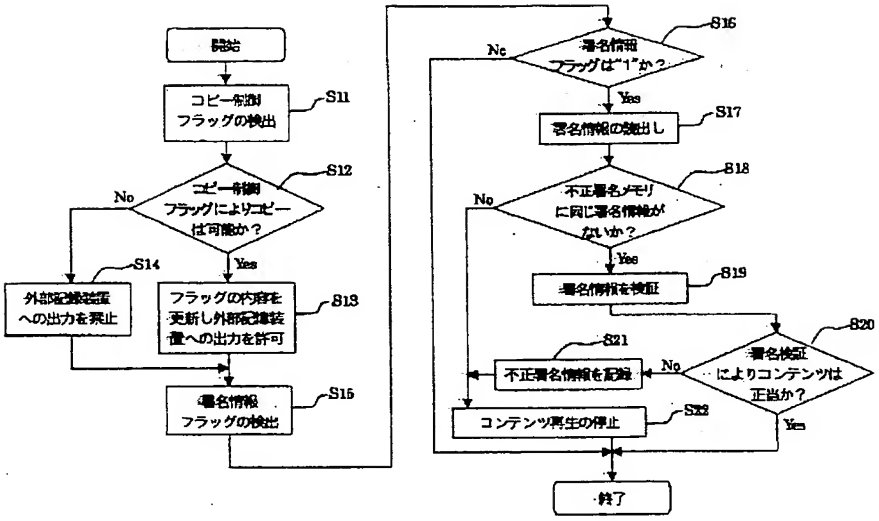
【図３】


開始
S1
コピー制御フラッグ設定がなされているか？
No
Yes
コピー制御フラッグ設定
S2
署名の設定
S3
ディジタルコンテンツ
署名情報
署名情報フラッグ
コピー制御フラッグ
の記録
S4
終了

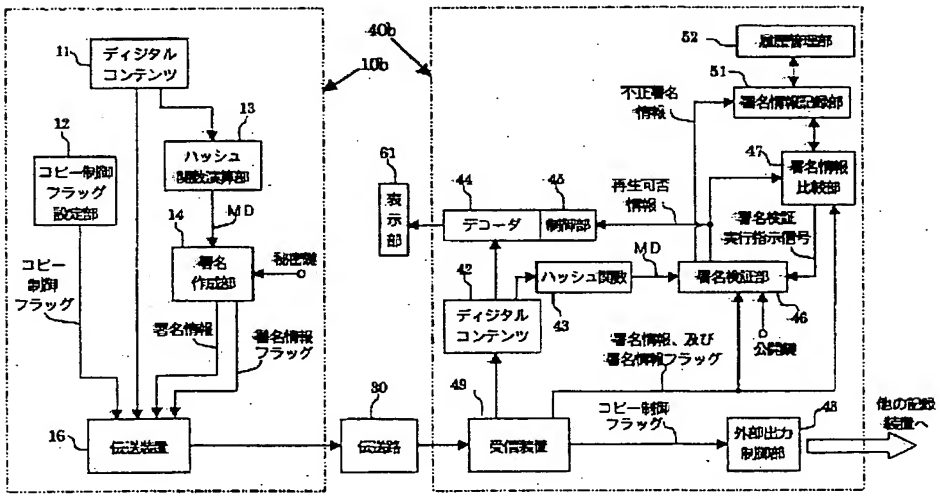
【図２】


11
ディジタルコンテンツ
12
コピー制御フラッグ設定部
18
ハッシュ関数演算部
14
MD
署名作成部
秘密鍵
コピー制御フラッグ
署名情報
署名情報フラッグ
15
信号記録部
40a
10a
20
ディジタルコンテンツ記録媒体
61
表示部
52
履歴管理部
51
不正署名情報
署名情報記憶部
47
署名情報比較部
44
45
再生可否情報
デコーダ
制御部
署名検証実行指示信号
42
ハッシュ関数
MD
署名検証部
ディジタルコンテンツ
43
46
公開鍵
署名情報、及び署名情報フラッグ
41
記録信号読み出し部
コピー制御フラッグ
48
外部出力制御部
他の記録装置へ

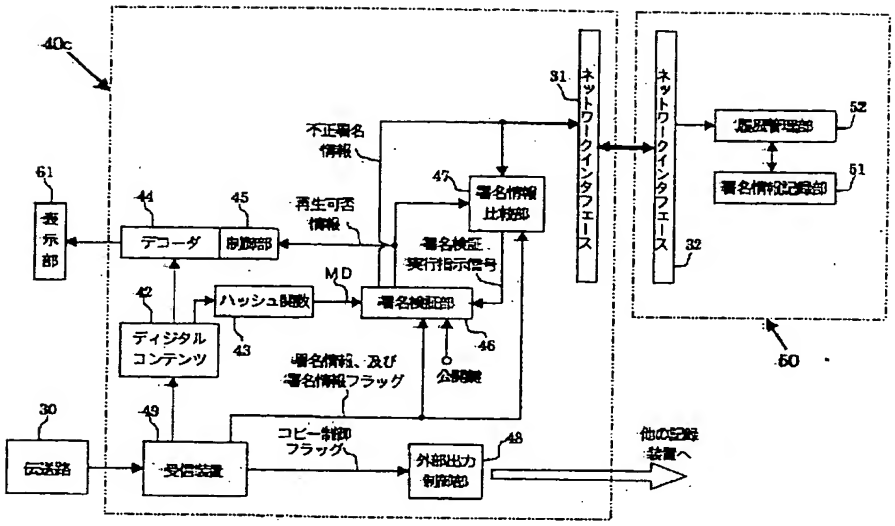
【図４】


開始
コピー制御フラグの検出
S11
コピー制御フラグによりコピーは可能か？
S12
No
Yes
外部記録装置への出力を禁止
S14
フラグの内容を更新し外部記録装置への出力を許可
S13
署名情報フラグの検出
S15
署名情報フラグは"1"か？
S16
No
Yes
署名情報の抽出し
S17
不正署名メモリに同じ署名情報がないか？
S18
No
Yes
署名情報を検証
S19
署名検証によりコンテンツは正当か？
S20
No
Yes
不正署名情報を記録
S21
コンテンツ再生の停止
S22
終了

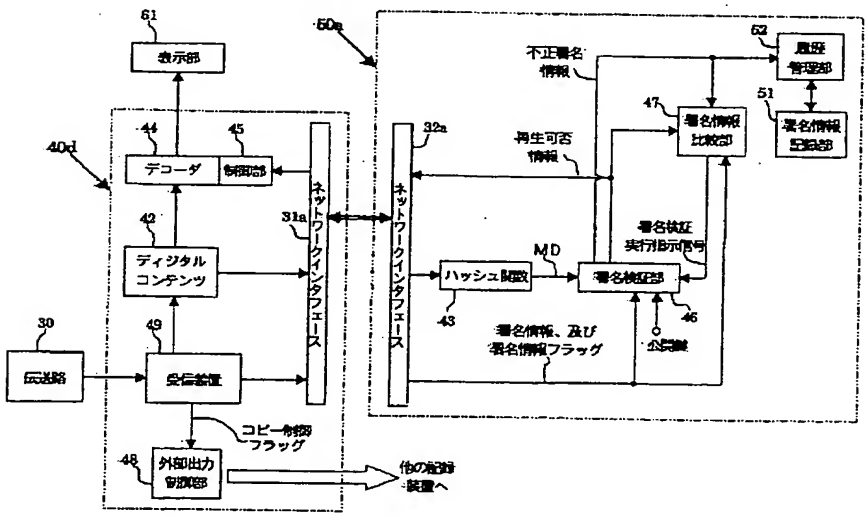
【図５】


11
ディジタルコンテンツ
12
コピー制御フラグ設定部
13
ハッシュ関数演算部
14
MD
署名作成部
秘密鍵
コピー制御フラグ
署名情報
署名情報フラグ
16
伝送装置
40b
10b
伝送路
30
61
表示部
44
デコーダ
45
制御部
再生可否情報
MD
ハッシュ関数
42
ディジタルコンテンツ
43
署名検証部
署名検証実行指示信号
署名情報、及び署名情報フラグ
公開鍵
46
47
署名情報比較部
51
署名情報記録部
不正署名情報
52
履歴管理部
49
受信装置
コピー制御フラグ
48
外部出力制御部
他の記録装置へ

【図６】



【図７】



フロントページの続き

Ｆターム(参考)　5B017 AA07 CA16
5C053 FA13 FA22 FA25 GA11 GB37
HA40 JA21
5J104 AA07 AA09 KA01